Barco

Wi-Fi and Security Considerations for ClickShare

Author

Guy Coen
guy.coen@barco.com

WI-FI CONSIDERATIONS

The right choice of frequencies and channels in larger scale Wi-Fi deployments requires thorough knowledge of RF (radio frequency) and Wi-Fi technology and appropriate tools like spectrum analyzers. However, a thorough treatment of that subject is beyond the scope of this white paper. In this paper, we provide some hints and tips that can be of help in smaller scale and non-critical installations. In all other cases, we strongly recommend that ClickShare be installed by professional integrators with thorough knowledge of RF and Wi-Fi technology.

- As the 2.4 GHz frequency band is usually already very crowded, and since ClickShare has 5 GHz capabilities, we recommend using the 5 GHz frequency band
- To choose an appropriate channel within the chosen frequency band (and among the allowed channels for the country concerned), we recommend using a Wi-Fi channel visualization tool like the freely available InSSIDer tool from MetaGeek, which is available on Windows and Mac OS/X platforms. This tool shows which channels are already occupied and which are not. Choose a channel that is still free (or that has weak signals from other APs).
- For each frequency band, ClickShare follows the country regulations in the channels offered. Every ClickShare Base Unit is factory set for a specific geographical region. Based on that setting, the administration interface offers only the legally allowed channels. Once the Base Unit has left the factory, the factory set region code cannot be changed. It is also not allowed to install a ClickShare Base Unit outside the region for which it is intended. This intended region is indicated in the article number at the bottom of the Base Unit: EU for Europe, NA for US and Canada, CN for China, JP for Japan. No such restrictions apply to the ClickShare Buttons.
- ClickShare does not automatically hop to other channels when there are changes in the RF environment. Therefore, we advise a regular check in environments where changes to Wi-Fi and other RF equipment are frequent.
- In most cases, your company's IT department will have a clear overview of the frequencies in use for different applications in different areas of the company. So, it is highly recommended to involve the IT department in your Wi-Fi deployment.

IEEE802.11N

ClickShare allows the use of IEEE802.11n, which has significant advantages compared to legacy wireless technologies – for example, it offers improved performance, coverage and robustness compared to older IEEE802.11 standards (IEEE802.11a/b/g). Another advantage is that it can use both the 2.4GHz and the (less crowded) 5GHz bands. However, it is still a wireless technology, so successful deployment requires careful planning based on a knowledge of the technology.

Key advantages of IEEE802.11n include:

- Frame aggregation: 802.11n boosts MAC (media access control) layer performance by allowing 802.11n devices to aggregate several packets into a single packet, which avoids the wasted overhead between frames.
- MIMO (multiple input, multiple output): this technology uses multiple antennas at both the transmitter and the receiver. MIMO exploits the fact that RF signals reflect off objects in their path, causing multi-path interference. MIMO transmits separate data streams at the same frequency but over different spatial channels (spatial multiplexing), thereby turning multipath into an advantage by making the channel more efficient.
- Channel bonding: in contrast to 802.11a and 802.11g, 802.11n can bond two 20MHz channels together to form a single 40MHz channel, which boosts the maximum throughput significantly.

Some legacy hardware sensors used in enterprise wireless intrusion detection systems (IDS) may not be able to detect 802.11n APs. The same applies for network management tools. Be sure that the spectrum analyzers that are used support MIMO spatial streams.

Real world performance depends on many factors, including environmental interference, system design, radio configuration, network design and building construction. We have designed ClickShare using best practices, but the environment always plays an important role. Factors that limit the performance of an IEEE802.11n system include:

- Legacy station support: 802.11n access points can be configured to interoperate with legacy IEEE802.11b/g/a devices. However, this reduces performance, because the legacy systems typically consume more "air time", so that the faster 802.11n endpoints must wait for the slower legacy systems before they can use the WLAN.
- Multi-path reflections: 802.11n uses multi-path reflections to its advantage. Therefore, environments with little or no multi-path reflections reduce IEEE802.11n's performance.
- No channel bonding: without channel bonding, the IEEE802.11n infrastructure is used below its full potential. Therefore, in the 5GHz band, IEEE802.11n can be

configured to use bonded non-overlapping 20MHz channels.

The following table compares the different IEEE802.11 standards:

	802.11b	802.11g	802.11a	802.11n
Maximum signaling rate	11 Mbps	54 Mbps	54 Mbps	300 Mbps
Operating frequency band	2.4 GHz	2.4 GHz	5 GHz	2.4 & 5 GHz
Typical range	100m	100m	100m	150m
Non-overlapping channels	3	3	23	3 (2.4 GHz) 23 (5 GHz)
Interference sources	Bluetooth, Microwave, Ovens, Baby monitors, etc	Bluetooth, Microwave, Ovens, Baby monitors, etc	Cordless phones	Same as IEEE802.11b/g at 2.4 GHz Same as IEEE802.11a at 5 GHz

OPERATIONAL MODES

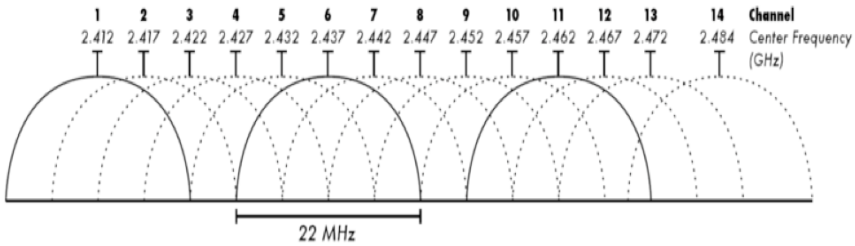
IEEE802.11n access points can be operated in multiple operational modes, each with advantages and disadvantages.

- **Mixed mode:** enables 802.11n devices to co-exist and interoperate with legacy 802.11b/g/a devices on the same WLAN.
- **Legacy mode:** makes the 802.11n AP behave like an 802.11g/a AP. There will be some performance improvements due to some physical layer enhancements, but the performance remains below full potential.
- **IEEE802.11n mode:** this provides maximum performance because the AP is not slowed down by more "air time"-consuming legacy devices.

CHANNEL SELECTION PER REGION

As stated above, the available channels vary according to the various regions of the world. ClickShare obeys these regulations and offers only those channels that are allowed in the region identified on the product label (see bottom of Base Unit, last 2 digits in the article number: e.g. NA for US and Canada, EU for Europe, etc.).

But potential interference from neighboring channels must also be considered. The 802.11 standard divides the frequency bands (2.4GHz and 5GHz) into channels. The 2.4GHz range is subdivided into 13 channels, each 22MHz wide and spaced 5MHz apart. These channels usually overlap one another, resulting in signal degradation. As shown in the figure below, there are only 3 non-overlapping channels available in the IEEE802.11 standard: channel 1 with centre frequency 2.412GHz, channel 6 with centre frequency 2.437GHz, and channel 11 with centre frequency 2.482GHz. Clearly, access points located near each other must avoid overlapping frequencies.



As we've said, a detailed description is beyond the scope of this white paper. We provide a simplified view to illustrate the

principle. For more complete information, please refer to the appropriate IEEE standards and local regulations.

Channels in the 2.4GHz frequency band

Channel	Frequency (MHz)	NA	JP	EU	CN
1	2412				
2	2417				
3	2422				
4	2427				
5	2432				
6	2437				
7	2442				
8	2447				
9	2452				
10	2457				
11	2462				
12	2467				
13	2472				

With 802.11g and newer standards, only channels 1, 5, 9, and 13 shall be used in order to obey the non-overlapping 20MHz OFDM channel scheme borrowed from 802.11a. But please survey the site first, and then if channel 6 is already heavily occupied, follow the 3-channel system.

Note that channels 12 and 13 are available in the US under low power conditions. However, since ClickShare's built-in AP does not support power adjustment, these two channels are blocked for US-designated Base Units.

Channels in the 5GHz frequency band

The picture for the 5GHz frequency band is more complex than that of the 2.4GHz band.

The United States requires that devices operating on 5.250–5.350 GHz and 5.470–5.725 GHz must employ dynamic frequency selection (DFS) and transmit power control (TPC)

capabilities in order to avoid interference with weather-radar and military applications. In 2010, the FCC further specified the use of channels in the 5.470–5.725 GHz band to avoid interference with Terminal Doppler Weather Radar (TDWR) systems. This eliminated the use of channels 120, 124, and 128. Channels 116 and 132 may be used, as long as they are separated by more than 30 MHz (center-to-center) from a TDWR located within 35 km of the device.

Germany requires dynamic frequency selection (DFS) and transmit power control (TPC) capabilities on 5.250–5.350 GHz and 5.470–5.725 GHz as well. In addition, the 5.150–5.250 GHz frequency range is allowed for indoor use only. As this is the German implementation of EU Directive2005/513/EC, similar regulations must be expected throughout the European Union.

Austria adopted Directive 2005/513/EC directly into national law.

South Africa copied the European regulations.

Japan allows channels 34, 38, 42, and 46 for connecting old APs supported by J52.

The following table gives an overview (valid at the time this document was being written) of the channels that are supported in at least one of ClickShare's target regions:

Channel	Frequency (MHz)	NA	EU	CN	JP
184	4920				
188	4940				
192	4960				
196	4980				
36	5180				
40	5200				
44	5220				
48	5240				
149	5745				
153	5765				
157	5785				

Channel	Frequency (MHz)	NA	EU	CN	JP
161	5805				
165	5825				

Important note: channel availability is also related to signal strength, which (among other things) is related to the antennas being used. If the user/integrator wishes to extend the Wi-Fi range by using larger antennas on the ClickShare Base Unit, Barco cannot guarantee that this configuration will still comply with the country regulations.

DYNAMIC FREQUENCY SELECTION

The ClickShare AP does not support DFS as specified in the IEEE802.h standard.

The 802.11h standard – commonly referred to as Dynamic Frequency Selection (DFS) – was created to define a set of procedures to detect and avoid interference with radar systems operating in the 5GHz range (UNII channels – 52-64 & 100-140). The part of the specification that is most visible to users is the ability of a DFS-capable AP to detect and move away from a channel that interferes with radar systems. APs that do not support DFS are not allowed to operate on the channels where interference occurs, which limits the number of channels available in the 5GHZ spectrum.

SIGNAL PROPAGATION IN THE REAL WORLD

The various mechanisms that affect the propagation of radio signals can be attributed to 5 main physical phenomena: reflection, diffraction, refraction, scattering and absorption (Hucaby, 2007; Durgin, et al, 1998; Sarkar, et al., 2003). These basic mechanisms distort the propagating signal (making the signal stronger or weaker), and they can also create additional propagation paths beyond the direct line of sight path between the radio transmitter and the receiver. This results in multiple signals reaching the receiver with different delays, causing shadowing and multi-path fading which affect performance.

In general, these phenomena depend on the surrounding environment and the frequency of the signal being used. Determining the effect of each of these phenomena for a given environment for a given frequency is a very complex task. As IEEE802.n uses MIMO, which involves multiple frequencies, the situation becomes even more complex.

Over the years, a number of mathematical radio propagation models have been developed to accurately predict the potential propagation of signals within an environment (Durgin, et al, 1998; Iskander & Yun, 2002; Mikas, et al., 2003; Garg, 2007). Basically, there are two approaches to modeling radio networks – the Empirical (or Statistical) method, and the Deterministic method:

- The empirical method is based on site survey and uses measurements gathered from the actual environment that is to be modeled.
- The deterministic method (also known as the Ray-Optical or Ray-Tracing model) uses software based on the theory of electromagnetic wave propagation.

Compared to the empirical site survey method, the deterministic method is usually more convenient and cost-effective. An optimal configuration can be reached by simulating different configurations of the environment in which the network will be deployed. However, an accurate prediction hereby depends on the availability of data such as the composition of the obstacles along the signal path and their corresponding effect on electromagnetic signals (Sarkar et al., 2003; Iskander & Yun, 2002; Mikas, et al., 2003). In such cases, site surveying is usually quicker and more accurate.

POWER OVER ETHERNET

The IEEE802.3af standard for power over ethernet (PoE) was developed to facilitate the deployment of WLAN APs in environments where it is difficult to access power. However, because it also drives the projector or display and performs video processing of the incoming video streams, ClickShare is more than a WLAN AP. Therefore, the ClickShare Base Unit does *not* include the PoE capability.

SSID BROADCASTING

We suggest that SSID broadcasting be switched off for normal use. Note that the factory activates SSID broadcasting to facilitate installation. It is then up to the integrator to switch it off for first use.

WLAN CONTROLLER

A WLAN controller is a device that provides centralized management and control of a collection of lightweight APs. The ClickShare Base Unit is neither a WLAN controller nor a lightweight AP, and so it cannot be operated as such.

RECOMMENDATIONS

ClickShare is a closed system and is not intended to interoperate with other, more general purpose, APs. Therefore, we strongly recommend the following:

- Use IEEE802.11n mode in the 5GHz frequency range,
- Set WPA2 protection with a strong password, and
- Switch off SSID broadcasting.

SECURITY CONSIDERATIONS

The security of a product or system can be viewed from several different angles. In the following sections, we cover various security concerns that people may have with ClickShare.

1. Introducing malware on the client PC
2. Tapping into content shown by ClickShare
3. ClickShare disturbing other parts of the IT environment
4. Secure management interfaces
5. External parties disturbing the meeting
6. Logging
7. Security benchmarking

INTRODUCING MALWARE ON THE CLIENT PC

The only software running on the client PC is the ClickShare Client software (the "Client"). This piece of software is developed and maintained in-house by Barco – no external party has access to this software. Furthermore, the binary software image is compressed and signed before it is sent to the factory that produces ClickShare.

The software is stored on a mass storage device inside the ClickShare Button which is read-only during normal use. It can only be programmed by the factory, or re-programmed by the ClickShare Base Unit (a normal user cannot write to this storage device, intentionally or unintentionally). In the case of re-programming, this is done by software running on the Base Unit, which is also developed and maintained in-house by Barco.

The software is *never* installed on a client PC (which affects permanent storage and configuration); it is merely run on that PC (which only affects volatile RAM memory and the CPU). The software does not require any special drivers to be installed on the PC and does not install any drivers itself.
Thus, it is virtually impossible for malware to enter the client PC through the ClickShare Button.

TAPPING INTO CONTENT SHOWN BY CLICKSHARE

No files are streamed or sent from the client PC to the ClickShare Base Unit – only the visual information as rendered locally on screen is transmitted through the ClickShare Button. The transmission of this visual information is done inside a WPA2-encrypted Wi-Fi channel.

Therefore, tapping into this information stream to recover the original data is virtually impossible.
Moreover, as the Base Unit is an endpoint for the stream, the information sent to the Base Unit is not sent back to any of the client devices.

CLICKSHARE DISTURBING OTHER PARTS OF THE IT ENVIRONMENT

ClickShare can have a number of interface points to the rest of the IT environment. However, ClickShare has been designed not to disturb other parts of the IT environment. The interface points are:

- Wired Ethernet port: used only for remote administration (not used for normal use of ClickShare). The Base Unit does not initiate any external connections over the Ethernet port. As an endpoint, it only opens a limited number of ports:
  - TCP port 80 (www): for administration through the web interface
  - TCP port 22 (ssh): for access by certified level 3 service technicians only
- Wi-Fi AP on the Base Unit: not intended as a general purpose AP, does no packet forwarding, is not a Wi-Fi controller or lightweight AP, is protected using (configurable) WPA2 encryption. The following ports are accessible through this interface:
  - TCP port 80 (www): for administration through the web interface
  - TCP port 22 (ssh): for access by certified level 3 service technicians only
  - TCP port 9876: for incoming connections from Buttons
  - TCP port 9870: provided for iPad support
  - TCP port 873 (rsync): for gathering Button log files on the Base Unit[1]
- Wi-Fi client on the ClickShare Button: limited by the firmware on the Button to connect only to the AP on the Base Unit, following the WPA2 encryption of the Base Unit.
- USB port on the Base Unit: it is advisable not to extend access to these USB ports through USB extenders beyond the physical boundaries of the meeting room. In normal use, these USB ports support only 3 devices:
  - ClickShare Button: used to pair the Button with that particular Base Unit, and to update the software residing on the Button. This process is handled entirely by server-side software running on the Base Unit.
  - USB pen drive: used to upgrade the software on the Base Unit itself. This process is handled entirely by server-side software running on the Base Unit. This software checks the content on the USB pen drive by verifying specific signatures (otherwise, no action is taken). Thus, it is impossible to change the Base Unit software by using a USB pen drive with malicious software.
  - Keyboard: used only by certified level 2 service technicians in case of problems. Because access is password protected, unauthorized persons cannot do anything via a connected keyboard.
- PHP: The Base Unit runs PHP 5.3.15 internally, which means that security vulnerabilities, if any, related to that PHP version also apply to the ClickShare Base Unit.

[1] In future versions of ClickShare, we plan to close the rsync port and replace it by syslog (UDP port 514).

SECURE MANAGEMENT INTERFACES

Administration of the Base Unit is done with a web browser via an HTTP interface[2]. The administrator logs on with a username + password. In addition to this, the Base Unit also accepts incoming SSH connections: the connection is SSL encrypted and authentication is performed with a username + password. The Base Unit does not place specific requirements on the passwords that are used: it is the administrator's responsibility to choose a password that is secure and difficult to hack[3].

EXTERNAL PARTIES DISTURBING THE MEETING

It is possible to abuse the system by taking a Button before a meeting starts and pairing it with the Base Unit in the meeting room in order to show unwanted content from outside the meeting room (within Wi-Fi range) during the meeting. We acknowledge this security weakness: it is the result of trading some security for greater ease of use.

Nevertheless, such abuse can easily be overcome by resetting the meeting room SSID or WPA2 password via the administration interface at the beginning of a critical meeting, and then pairing only the Buttons present in the meeting room during the meeting. This is why we strongly recommend not extending access to the Base Unit USB ports beyond the physical boundaries of the meeting room. Also, note that each additional Button that shares content with the Base Unit reveals the user on the central screen (i.e., the name of the user as read from the operating system configuration).

LOGGING

The ClickShare system contains an extensive logging engine (primarily using syslog) – each individual Button has a local log file that logs operations executed on that particular Button, the Base Units it has already been paired with, etc. The Base Unit collects the log files from the Buttons connected to it. It also has its own log file, which contains all Button actions as well as administrator manipulations performed on the Base Unit.

[2] In future versions, this will be replaced by the more secure HTTPS.
[3] In future versions, to guard the system from being hacked by dictionary trials, the Base Unit will not accept passwords that do not fulfill certain minimum requirements. After 3 false attempts, the administration interface will be blocked for 24 hours.

REFERENCES

[1] "Silent Film Speed". Cinemaweb.com

[2] "Cameron, Showscan, and 3-D". Mkpe.com

[3] "A movie lover's plea: Let there be light". Boston Globe, 22/05/2011